

QUANTUM HASHING. GROUP APPROACH

M. ZIATDINOV

ABSTRACT. In this paper we consider a generalization of quantum hash functions for arbitrary groups. We show that quantum hash function exists for arbitrary abelian group. We construct a set of “good” automorphisms — a key component of quantum hash function. We prove some restrictions on Hilbert space dimension and group used in quantum hash function

1. INTRODUCTION

Buhrman et al. in [3] introduced the notion of quantum fingerprinting and constructed first quantum hash function. Ablayev and Vasiliev in [1] offered another version of quantum fingerprinting.

In [2] construction of Buhrman et al. and Ablayev-Vasiliev’s construction are generalized. It is shown that both approaches can be viewed as composition of “quantum generator” and (classical) universal hash function. Also the notion of “quantum hash function” is introduced.

We present an algebraic generalization of Ablayev-Vasiliev’s construction. Main reason of it is maximal abstraction while retaining such properties of quantum hash function as simple evaluation, ability to continue computing hash (i.e. hash value of string concatenation can be somehow evaluated based on hash of first string and second string), simple reverse transform (in Ablayev-Vasiliev’s construction it is enough to reverse input string and change the sign of rotations).

In section 2 required definitions are introduced, sections 3-5 are devoted to construction of quantum hash function for arbitrary abelian group, section 6 proves existence of “good” automorphisms which are key component of quantum hash function, section 7 is devoted to some restrictions on possible combinations of parameters of quantum hash function.

2. DEFINITION

We start with recalling basic definitions that we will need in the paper

Let x be a n -bit message: $x \in \{0, 1\}^n$.

Let us consider functions mapping $\{0, 1\}^n$ to some (arbitrary finite) group G with group operation \circ and unit element e :

$$h : \{0, 1\}^n \rightarrow G$$

Let us choose a homomorphism $f : G \rightarrow [(\mathcal{H}^2)^{\otimes m} \rightarrow (\mathcal{H}^2)^{\otimes m}]$, i.e. function that preserves group structure:

$$f(g_1 \circ g_2) = f(g_1)f(g_2).$$

We use $[(\mathcal{H}^2)^{\otimes m} \rightarrow (\mathcal{H}^2)^{\otimes m}]$ notation for a set of all unitary transformations on m qubits.

Let us choose a set of automorphisms \mathbb{K} from group of all automorphisms $\text{Aut}(G)$:

$$(1) \quad k_i \in \mathbb{K} \subseteq \text{Aut}(G), \quad 1 \leq i \leq T.$$

We will use notation $k\{g\}$ for image of g under automorphism k .

We generalize notion introduced in [1] as follows. We call set K_{good} of elements of chosen \mathbb{K} “good” set if for each non-unit group element g :

$$(2) \quad \forall g \in G, g \neq e : \frac{1}{|K_{\text{good}}|^2} \left| \sum_{k \in K_{\text{good}}} \langle \psi_0 | f(k\{g\}) | \psi_0 \rangle \right|^2 < \epsilon$$

Let us also require that for each group element:

$$(3) \quad \forall g \in G : \mathbf{E}_{k \in \mathbb{K}} \left[\langle \psi_0 | f(k\{g\}) | \psi_0 \rangle \right] = 0$$

In section 6 we will show that this requirement involves existence of “good” set K_{good} of elements of \mathbb{K} . Also we will show that this set can be chosen randomly with high probability

In the remaining part of this section we will consider that “good” subset $K_{\text{good}} = \{k_1, \dots, k_t\}$ is constructed and its elements are some automorphisms $k_j \in \mathbb{K}, 1 \leq j \leq t$.

Let us define quantum hash function as follows.

Definition 1. *Quantum hash function based on classical hash function h mapping X^n to group G , “good” set of automorphisms $K = \{k_0, \dots, k_{t-1}\}$ and homomorphism f to space $[(\mathcal{H}^2)^{\otimes m} \rightarrow (\mathcal{H}^2)^{\otimes m}]$:*

$$|\Psi_{h,G,K,f,m,|\Psi_0\rangle}(x)\rangle = \frac{1}{\sqrt{t}} \sum_{j=0}^{t-1} \left(|j\rangle \otimes f(k_j\{h(x)\}) | \psi_0 \rangle \right).$$

We need homomorphism and automorphisms here, because we want to preserve group structure. It will allow us easily compute hash of string concatenation and invert quantum hash function: e.g. to compute hash of string concatenation one need to compute hash of first string and feed it as initial state to second string's hash computation:

$$|\Psi_{h,G,K,f,m,|\Psi_0\rangle}(u \cdot v)\rangle = |\Psi_{h_1,G,K,f,m,|\Psi_1\rangle}(v)\rangle,$$

where h can be represented as $h(u \cdot v) = h(u) \circ h(v)$, and

$$|\Psi_1\rangle = |\Psi_{h,G,K,f,m,|\Psi_0\rangle}(u)\rangle.$$

To reverse quantum hash function one need to negate $h(x)$.

In the rest of the article we will omit $|\Psi_0\rangle$ parameter if its value is clear from the context.

Let us consider square of scalar product of quantum hash function values on different inputs:

$$\begin{aligned} & |\langle \Psi_{h,G,K,f,m}(x) | \Psi_{h,G,K,f,m}(x') \rangle|^2 = \\ & = \left| \frac{1}{t} \sum_{j=0}^{t-1} \left(\langle j|j \rangle \langle \psi_0 | f^\dagger(k_j\{h(x)\}) f(k_j\{h(x')\}) | \psi_0 \rangle \right) \right|^2 = \\ & = \left| \frac{1}{t} \sum_{j=0}^{t-1} \langle \psi_0 | f(k_j\{h^{-1}(x) \circ h(x')\}) | \psi_0 \rangle \right|^2 \end{aligned}$$

If hash function h has no collision, and $h(x) \neq h(x')$, product $h(x') \circ h(x)^{-1}$ will be equal to some element $g \neq e$ of group G , and by definition of “good” subset K_{good} square of scalar product will be equal to:

$$\left| \frac{1}{t} \sum_{j=0}^{t-1} \langle \psi_0 | f(k_j\{h^{-1}(x) \circ h(x')\}) | \psi_0 \rangle \right|^2 < \epsilon.$$

Otherwise, square of scalar product equals to one:

$$\begin{aligned} & \left| \frac{1}{t} \sum_{j=0}^{t-1} \langle \psi_0 | f(k_j\{h^{-1}(x) \circ h(x')\}) | \psi_0 \rangle \right|^2 = \left| \frac{1}{t} \sum_{j=0}^{t-1} \langle \psi_0 | f(k_j\{e\}) | \psi_0 \rangle \right|^2 = \\ & = \left| \frac{1}{t} \sum_{j=0}^{t-1} \langle \psi_0 | f(e) | \psi_0 \rangle \right|^2 = \langle \psi_0 | f(e) | \psi_0 \rangle = \langle \psi_0 | \psi_0 \rangle = 1 \end{aligned}$$

3. EXAMPLE: \mathbb{Z}_q

Fingerprinting technique suggested in [1] can be considered as special case of described scheme. In other words,

Lemma 1. *There exists quantum hash function for \mathbb{Z}_q group, some set of automorphisms K_{good} and homomorphism into $(\mathcal{H}^2)^{\otimes m}$ space.*

We will use \mathbb{Z}_q as group G and $x \bmod q$ as hash function $h(x)$.

Required homomorphism $f(g)$ of group G into space $(\mathcal{H}^2)^{\otimes 1}$ is qubit rotation around Y axis on $\frac{2\pi g}{q}$ angle. It is homomorphism, because product of two rotations on angle $\frac{2\pi g}{q}$ and on angle $\frac{2\pi g'}{q}$ is rotation on angle $\frac{2\pi(g+g')}{q}$, where sum is modulo q , i.e. in \mathbb{Z}_q group.

The group of automorphisms of \mathbb{Z}_q group is \mathbb{Z}_q^\times group:

$$\text{Aut}(\mathbb{Z}_q) = \mathbb{Z}_q^\times.$$

So, we choose $\mathbb{K} \subseteq \text{Aut}(G)$ to be a set of multiplications to \mathbb{Z}_q^\times elements. It is easy to show that condition (3) holds:

$$\forall g \in \mathbb{Z}_q : \mathbf{E}_{k \in \mathbb{Z}_q^\times} \left[\left| \exp \left\{ \frac{2\pi k g}{q} \right\} |0\rangle \right| \right] = 0$$

4. EXAMPLE: $G_1 \times G_2$ GROUP

Elements of group $G_1 \times G_2$ are pairs of corresponding group elements. Group operation is defined component-wise:

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2)$$

Unit element is pair (e_1, e_2) of corresponding group units.

Let f_1 and f_2 be homomorphisms from G_1 to $(\mathcal{H}^2)^{\otimes m_1}$ and from G_2 to $(\mathcal{H}^2)^{\otimes m_2}$, correspondingly. Let $\mathbb{K}_1 \subseteq \text{Aut}(G_1)$ and $\mathbb{K}_2 \subseteq \text{Aut}(G_2)$ be corresponding automorphisms that satisfy condition 3.

Let us define homomorphism f from $G = G_1 \times G_2$ to $(\mathcal{H}^2)^{\otimes (m_1+m_2)}$ as follows:

$$f((g_1, g_2)) = f_1(g_1) \otimes f_2(g_2).$$

Let us choose automorphism set $\mathbb{K} \subseteq \text{Aut}(G)$ as follows:

$$\mathbb{K} = \{(g_1, g_2) \mapsto (k_1\{g_1\}, k_2\{g_2\}) : k_1 \in \mathbb{K}_1, k_2 \in \mathbb{K}_2\}.$$

Let us show that condition (3) is satisfied for this set, if it is satisfied for \mathbb{K}_1 and \mathbb{K}_2 :

$$\begin{aligned}
\mathbf{E}_{k \in \mathbb{K}} \left[|f(k\{g\})|0\rangle| \right] &= \mathbf{E}_{(k_1, k_2) \in \mathbb{K}_1 \times \mathbb{K}_2} \left[f_1(k_1\{g_1\})|0\rangle \otimes f_2(k_2\{g_2\})|0\rangle \right] = \\
&= \frac{1}{|\mathbb{K}_1|} \sum_{k_1 \in \mathbb{K}_1} \left(\frac{1}{|\mathbb{K}_2|} \sum_{k_2 \in \mathbb{K}_2} f_1(k_1\{g_1\})|0\rangle \otimes f_2(k_2\{g_2\})|0\rangle \right) = \\
&= \frac{1}{|\mathbb{K}_1|} \sum_{k_1 \in \mathbb{K}_1} f_1(k_1\{g_1\})|0\rangle \cdot \frac{1}{|\mathbb{K}_2|} \sum_{k_2 \in \mathbb{K}_2} f_2(k_2\{g_2\})|0\rangle = \\
&= \mathbf{E}_{k_1 \in \mathbb{K}_1} \left[f_1(k_1\{g_1\})|0\rangle \right] \cdot \mathbf{E}_{k_2 \in \mathbb{K}_2} \left[f_2(k_2\{g_2\})|0\rangle \right] = 0
\end{aligned}$$

Thus, holds

Lemma 2. *If there exists quantum hash functions for G_1, G_2 groups in $(\mathcal{H}^2)^{\otimes m_1}$ and $(\mathcal{H}^2)^{\otimes m_2}$ spaces with f_1 and f_2 homomorphisms and \mathbb{K}_1 and \mathbb{K}_2 automorphism sets satisfying 3, correspondingly, we can define quantum hash function for $G_1 \times G_2$ in $(\mathcal{H}^2)^{\otimes (m_1+m_2)}$ space.*

5. EXAMPLE: ARBITRARY ABELIAN GROUPS

Theorem 1. *For arbitrary abelian group G there exists quantum hash function with some automorphism set K_{good} and homomorphism f .*

We can decompose every abelian group G as follows:

$$G = \mathbb{Z}_{p_1^{\sigma_1}} \otimes \cdots \otimes \mathbb{Z}_{p_t^{\sigma_t}},$$

thus we can apply lemma 1 to define quantum hash function in each of $\mathbb{Z}_{p_1^{\sigma_1}}, \dots, \mathbb{Z}_{p_t^{\sigma_t}}$ groups, and then apply lemma 2 to compose these hash functions to hash function for G .

6. “GOOD” AUTOMORPHISM SUBSETS

In this section we will consider that homomorphism $f : G \rightarrow [(\mathcal{H}^2)^{\otimes m} \rightarrow (\mathcal{H}^2)^{\otimes m}]$ and automorphism set \mathbb{K} are chosen:

$$k_i \in \mathbb{K} \subseteq \text{Aut}(G), \quad 1 \leq i \leq T,$$

such that for each group element holds:

$$\forall g \in G : \mathbf{E}_{k \in \mathbb{K}} \left[\langle \psi_0 | f(k\{g\}) | \psi_0 \rangle \right] = 0$$

Then holds

Theorem 2. *For random set K of elements of set \mathbb{K} (each element is chosen uniformly at random from \mathbb{K}) the probability of K being “bad” for some g does not exceed $1/|G|$:*

$$\mathbf{P}\left(\frac{1}{|K_{\text{good}}|^2} \left| \sum_{k \in K_{\text{good}}} \langle \psi_0 | f(k\{g\}) | \psi_0 \rangle \right|^2 \geq \epsilon\right) \leq \frac{1}{|G|}$$

Proof. Let us consider random variables

$$X_i = \langle \psi_0 | f(k_i\{g\}) | \psi_0 \rangle,$$

where $\{k_1, k_2, \dots, k_t\} = K$, and

$$Y_t = \sum_{i=1}^t X_i.$$

Let us show that sequence $Y_0 = 0, Y_1, Y_2, \dots, Y_{|K|}$ is a martingale (cf. [4]).

Let us show that expectation value of Y_t exists and is finite.

$$(4) \quad \mathbf{E}[Y_t] = \sum_{i=1}^t \mathbf{E}[X_i] = \sum_{i=1}^t \mathbf{E}[\langle \psi_0 | f(k_i\{g\}) | \psi_0 \rangle] = 0$$

Let us show that conditional expectation of Y_t given Y_{t-1}, \dots, Y_1, Y_0 is equal to Y_{t-1} :

$$(5) \quad \mathbf{E}[Y_t | Y_{t-1}, \dots, Y_0] = \frac{1}{|K|} \sum_{i=1}^{|K|} (Y_{t-1} + \langle \psi_0 | f(k_i\{g\}) | \psi_0 \rangle) = Y_{t-1} + \mathbf{E}[X_i] = Y_{t-1}$$

Because (4) and (5) hold, Y_t is a martingale.

Let us estimate the difference of Y_t and Y_{t-1} :

$$|Y_t - Y_{t-1}| = \left| \sum_{i=1}^t X_i - \sum_{i=1}^{t-1} X_i \right| = |X_t| \leq 1$$

Let us apply Azuma inequality:

$$(6) \quad \mathbf{P}(|Y_{|K|} - Y_0| > \lambda) = \mathbf{P}\left(\left| \sum_{i=1}^{|K|} X_i \right| > \lambda\right) \leq 2 \exp\left\{-\frac{\lambda^2}{2|K|}\right\}$$

Let

$$\lambda = \sqrt{\epsilon}|K|.$$

Then Azuma inequality (6) will take the form:

$$\mathbf{P}\left(\left| \sum_{i=1}^{|K|} X_i \right| > \sqrt{\epsilon}|K|\right) \leq 2 \exp\left\{-\frac{\epsilon|K|^2}{2}\right\} \leq \frac{1}{|G|}$$

where $|K| \geq \frac{2}{\epsilon} \ln |G|$.

This inequality means that set K is not “good” for *some* g .

Thus, probability of set K not being “good” *at least for some* non-unit g does not exceed $(|G| - 1)/|G|$.

So, “good” automorphism set exists with probability of $1/|G|$. \square

7. ON DIMENSION OF SUBSPACES AND GROUP IN QUANTUM HASH FUNCTION

Definition 2. *A complex reflection is non-trivial element that fix a complex hyperplane in space pointwise. A p -fold reflection matrix has characteristic roots 1 (repeated $n - 1$ times) and θ , a primitive p -th root of unity (cf. [5]).*

Definition 3. *Unitary group generated by reflections (u.g.g.r.) — any finite group acting on a finite-dimensional complex vector space that is generated by complex reflections.*

The unitary groups generated by reflections were classified by Shephard and Todd in [6].

Let us have quantum hash function:

$$|\Psi_{h,G,K,f,m}(x)\rangle$$

Because of Shephard and Todd result group G and dimension m cannot be arbitrary: group must be subgroup of product of u.g.g.r., and dimension cannot be less than minimal product of dimensions of corresponding u.g.g.r.

In other words, holds

Theorem 3. *In arbitrary quantum hash function $|\Psi_{h,G,K,f,m}(x)\rangle$ group G is subgroup of some product of u.g.g.r. in $(\mathcal{H}^2)^{\otimes m}$; and vice versa, dimension m cannot be less than dimension of space in which such product of u.g.g.r. can exist.*

E.g., let we want to construct quantum hash function in which classical hash function maps input to some permutation on k points. Then it is impossible to find homomorphism into space with dimension less than k .

Proof. Let us prove that group G must be subgroup of product of u.g.g.r.

Let group G consists of g_1, g_2, \dots, g_t . Because group is finite, there is some r that is group order:

$$g_i^r = e$$

Because $f(g_i) = U_i$ is a unitary matrix, its characteristic roots are some r -th roots of unity:

$$f(g_i)^r = f(g_i^r) = f(e) = E$$

Thus each of U_i can be represented in form:

$$U_i = V_i^T A_{i0} A_{i1} A_{is_i} V_i,$$

where A_{ij} is some reflection matrix, and V_i is some unitary matrix.

All elements of form $V_i^T A_{ij} V_i$ are some reflections in unitary space and are elements of some u.g.g.r. \square

REFERENCES

- [1] Ablayev, F.; Vasiliev, A. Algorithms for quantum branching programs based on fingerprinting. *Electronic Proceedings in Theoretical Computer Science* 9: 1–11, 2009.
- [2] Ablayev, F.; Vasiliev, A. Cryptographic quantum hashing. *Laser Physics Letters* 11.2, 2014.
- [3] Buhrman, H.; Cleve, R.; Watrous, J.; De Wolf, R. Quantum fingerprinting. *Physical Review Letters*, 87(16), 2001.
- [4] McDiarmid, C. On the method of bounded differences. *Surveys in combinatorics*, 1989.
- [5] Shephard, G.C. Unitary groups generated by reflections. *Canadian J. Math.*, **5.3**: 363–383, 1953.
- [6] Shephard, G.C.; Todd, J.A. Finite unitary reflection groups. *Canadian J. Math.*, **6.2**: 274–304, 1954.